

Support and Incident Management Policy

Bonfire Interactive Ltd. | Confidential

Table of Contents

Purpose of Document	3
Downtime.....	3
Solution Maintenance.....	3
Solution Patches.....	3
Communication Standards	3
Definitions	3
Core Business Hours.....	3
Holidays	3
Incident Response Standards	4
Event Notification	4
Support Performance	4
Tier 1 Incidents.....	4
Tier 2 Incidents.....	5
Tier 3 Incidents.....	5
Support Requests	5
Maintenance Windows and Service Notifications	5
Unplanned Event Notification	6
Privacy and Security Incident Response	6
How to Report an Incident	6
Severity.....	6
Internal Issues	7
Compromised Communications	7
Response Steps.....	7
Response Meeting – Agenda.....	7
External Notifications.....	8
Mitigation	8
Documentation	8
Disaster Recovery and Service Recovery	8
Disaster Recovery	8
Service Recovery.....	9
Insurance	9

Purpose of Document

This document details Bonfire's support and incident management policy and processes for dealing with customer support, privacy and security, maintenance, and disaster recovery. The document serves as (1) an internal guide for Bonfire staff in managing these activities, and (2) a clear and understandable service level commitment for customers.

Key Definitions

Downtime

Complete unavailability of web portal or API to the user as measured at the Bonfire platform's internet access point. Network unavailability from user to the web server is not included. Downtime may be planned (as in the case of maintenance) or unplanned (as in the case of disaster). An outage must persist for more than 15 minutes to be considered downtime.

Solution Maintenance

Includes major maintenance activities, improvements, and/or upgrades to core platform and/or features. May require downtime. May cause changes in how a customer operates business processes / workflows in Bonfire.

Solution Patches

Includes minor maintenance activities, improvements, and/or upgrades to core platform and/or features. Does not require downtime. Does not cause changes in how a customer operates business processes / workflows in Bonfire.

Communication Standards

This defines the communication standards which Bonfire will commit to.

Definitions

Core Business Hours

Core business hours are 8:00 a.m. to 8:00 p.m. EST/EDT (UTC-5, UTC-4 during daylight savings), Monday through Friday. All durations in this document are in business hours/days.

Holidays

Public holidays are not considered a part of core business hours. Such holidays are not included in any durations in this document.

Incident Response Standards

The following standards apply to the response to and handling of incidents impacting customers.

Level		Incident A	Incident B	Incident C
Response Within	Initial Response	1 hour	1 hour	1 hour
	Start Work	2 hours	4 hours	1 day
	Resolution	2 days	3 days	4 days
Compliance Target		100%	100%	100%
Communication Methods		Email to the primary contact notifying of the incident and process to resolve. Phone available for follow up communication.		
		Email and phone to primary contact for Organizations with opportunities closing within 3 days. Organizations will be contacted in order of project close date (most immediate close date first).		

Event Notification

The following standards apply to notification of events that have happened or will happen.

Level	Planned A	Planned B	Planned C	Unplanned A
Response	1 week prior	3 days prior	1 day prior	3 days after
Compliance Target	100%	100%	100%	100%
Communication Methods	Email to the primary contact notifying of the event. Phone available for follow up communication.			

Support Performance

Tier 1 Incidents

Tier 1 incidents have a major impact on customer ability to operate entire business processes. No work-around or manual process is available.

Communication Standard: Incident Response Level A

Tier 2 Incidents

Tier 2 incidents include minor system or component failure or malfunction causing impact on customer ability to operate significant business processes. No work-around or manual process is available.

Communication Standard: Incident Response Level B

Tier 3 Incidents

Tier 3 incidents include component failure or malfunction not causing impact on customer ability to operate significant business processes. Work-around or manual processes are available.

Communication Standard: Incident Response Level C

Support Requests

Customer support requests not relating to an incident will be responded to promptly. Start work and resolution times are dependent on the nature of the request.

Communication Standard: Incident Response Level C (for initial response only)

Maintenance Windows and Service Notifications

Bonfire will provide notification of planned maintenance and service depending on the impact to the customer and the duration of impact.

Maintenance Type	Communication Standard
Planned emergency outage.	Event Notification - Planned C
Planned emergency maintenance including but not limited to urgent patches.	Event Notification - Planned C
Regular maintenance (requiring downtime) including but not limited to defect fixes, software patches and hardware maintenance. Downtime of 4 hours or less.	Event Notification - Planned B
Regular maintenance (requiring downtime) including but not limited to defect fixes, software patches and hardware maintenance. Downtime of more than 4 hours.	Event Notification - Planned A

All solution maintenance shall be performed outside of core business hours and be no longer than 8 hours in duration. All solution patches may be performed during core business hours, without advance notice to the customer.

Unplanned Event Notification

Bonfire may need to communicate events to customers that were not planned. Such events may include, but are not limited to, the following:

- Emergency maintenance
- Internet/network outages beyond Bonfire's control affecting the Bonfire application
- Unplanned service degradation
- Natural Disasters affecting the Bonfire application

Communication Standard: Unplanned A

Privacy and Security Incident Response

This section offers guidance for employees or incident responders who believe they have discovered or are responding to a security incident.

How to Report an Incident

Below are ways to report a security incident:

- Email security@gobonfire.com
- Message #general, #it, or #security on Slack.
- Create an IT service desk incident ticket - <https://bonfirehub.atlassian.net/servicedesk/customer/portals>
- Contact your manager

It is important to include as many specifics and details as you can.

Severity

Severity Level	Description	Examples	Action
Low or Medium	Most issues fall under this category. These do not require someone to be paged or woken up in the middle of the night.	Suspicious emails, outages, strange activity on a laptop	Ping slack channel and create a JIRA ticket
High	These are problems where an adversary or active exploitation hasn't been proven yet, and an attack may	malware, malicious access of business data (e.g. passwords, payment information,	Ping slack channel with @channel and create a JIRA ticket

	not have happened, but is likely to happen.	vulnerability data, etc.)	
Critical	The attackers were successful, and something was lost.		Ping slack channel with @channel, create a JIRA ticket, follow escalation procedures to CTO & CEO until acknowledged.

Internal Issues

When the malicious actor is an employee, contractor, vendor, or partner, please contact the Security team directly (or CEO, CTO, COO, Director of Security). Do not discuss the issue with other employees without permission from Bonfire leadership.

Compromised Communications

If there are IT communication risks (i.e. company phones, laptops, email accounts, etc. are compromised) the team will announce an out-of-band communication tool within the office.

Response Steps

For critical issues, the response team will follow an iterative response process designed to investigate, contain the exploitation, remediate the vulnerability, and capture postmortem or lessons learned elements.

1. Bonfire senior leadership should determine if a lawyer should be involved with attorney-client privilege
2. Additional individuals will be included as necessary as to keep the details of the incident on a need to know basis.
3. A “War Room” will be designated.
4. Notifications and release of details internally will be controlled as to ensure facts are released and rumors with misinformation do not propagate.
5. The following meeting will take place at regular intervals, starting with twice per day, until the incident is resolved

Response Meeting – Agenda

- Update the Breach Timeline with all known data related to the incident. The timeline should detail what you’re sure the attacker did at what times.

- Review new Indicators of Compromise with the entire group. Indicators of Compromise are anything you know belongs to the attacker: an IP address that sent data, a compromised account, a malicious file used to spearphish, etc.
- Add new data (knowns and unknowns) to the Investigative Q&A, which is a list of questions to which, if you had answers, you'd understand everything the attacker did.
- Update the list of Emergency Mitigations: passwords to be reset, laptops to be wiped, IPs to be banned, etc.
- Long Term Mitigations (including Root Cause Analysis): record everything you'll start doing so this crisis doesn't happen again.
- Everything Else: communications, legal issues, blog posts, status pages, etc.

External Notifications

In the event of a security or privacy breach, Bonfire will notify the affected parties.

In the case of a breach involving organizational data, organization contacts or affected organizations will be notified.

In the case of a personal data breach, the affected individuals will be contacted.

Communication of any such event will describe the nature of the event, the information affected, likely consequences, measures that Bonfire will take, and any recommended actions the affected parties should take.

Mitigation

In the event of a privacy or security breach Bonfire will ensure that any compromised user account(s) are disabled or passwords rotated immediately as they are identified after a breach is discovered.

Documentation

Bonfire will provide documentation explaining the breach, its impact, and steps that were taken in response to the breach. Supporting artifacts are to be captured and saved.

Disaster Recovery and Service Recovery

This section provides service level guidelines in the event of a Disaster Recovery or Service Recovery scenario.

Disaster Recovery

Requirement	Expected Service Level Value
Bonfire will ensure the mean time to recovery from an	Four (4) hours

unplanned outage will be within the following period:	
Bonfire will ensure that the solutions recovery time objective (RTO) allowing the solution users return to operations will be as follows:	The recovery time objective will be 1 day. Critical business functions will be resumed within 24 hours of disaster. Necessary business functions will be resumed immediately following the resumption of critical functions but no longer than 7 elapsed days. Desirable functions shall be resumed immediately following the resumption of necessary function, but no longer than 30 elapsed days following a disaster.
Bonfire will ensure that the recovery point objective (RPO) will be as follows:	The recovery point objective will be two (2) hours. The recovery point is defined at the time between the disaster event and the historical point to which data will be restored.

Service Recovery

Requirement	Expected Service Level Value
Bonfire will ensure that after any service disruption, security breach, or other event that may impact the integrity of customer data, the solution recovery period to restore/clean/restart compromised system and data to last point of integrity will be as follows:	8 hours for tier 3 incidents, 24 hours for tier 2 incidents and 48 hours for tier 1 incidents.

Insurance

Bonfire has insurance in place in case of disruption or disaster. Insurance is through Berkley Insurance Company with policy number BC02293.